UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION	))	MDL No. 1:19md2915 (AJT/JFA)

AMAZON'S MEMORANDUM IN SUPPORT OF MOTION TO FILE UNDER SEAL AND NOTICE OF INTENT TO REQUEST REDACTION OF TRANSCRIPT

Defendants, Amazon.com, Inc., and Amazon Web Services, Inc. (together, "Amazon"), by counsel and pursuant to Local Civil Rule 5 of Local Rules for the United States District Court for the Eastern District of Virginia, files this Memorandum in Support of Amazon's Motion to File Under Seal pursuant to the Court's October 4, 2021 order regarding the September 30, 2021 hearing transcript, Dkt. 2030. Amazon moves to file under seal the following ("Excerpts") from the September 30, 2021 hearing transcript: 72:10-14; 101:8-12; 211:6-13; 215:19-24; and 248:23-249:13.

These Excerpts should be sealed because they discuss a highly sensitive threat intelligence gathering practice that has been designated as "Confidential" or "Confidential – Outside Counsel Only" pursuant to the terms of the Amended Stipulated Protective Order, Dkt. 368. The usefulness of the threat intelligence practice would be compromised if the information contained in the Excerpts were revealed to the public.

I. THE PROCEDURAL REQUIREMENTS FOR SEALING HAVE BEEN MET.

Under the local rules of this Court, a party may file a motion to seal together with the proposed sealed filings. Local Civ. R. 5(C). The Court will subsequently determine whether the sealing or redactions are proper. The Court has also provided instructions to request redaction of a hearing transcript in its minute order. Dkt. 2030.

A "trial court has supervisory power over its own records and may, in its discretion, seal documents if the public's right of access is outweighed by competing interests." *In re Knight Publ'g Co.,* 743 F.2d 231, 235 (4th Cir. 1984). Before documents within a case may be filed under seal in the Fourth Circuit, the parties must: (1) provide notice to the public and give the public an opportunity to object to the sealing; (2) consider less drastic alternatives; and (3) provide specific findings in support of the decision to seal and the rejection of alternatives. *Ashcraft v. Conoco, Inc.*, 218 F.3d 282, 288 (4th Cir. 2000). All of these prerequisites are satisfied here.

First, the Court must provide notice of a request for sealing in the court record and provide interested persons with "an opportunity to object." *In re Knight*, 743 F.2d at 235. The Court does not need to provide notice to the public of each document to be sealed where such individual notice would be "impractical" and "unwarranted," as is the case here. *Id.* It is sufficient to docket the notice "reasonably in advance of deciding the issue." *Id.* In accordance with Local Civil Rule 5, Amazon's sealing motion was publicly docketed, with a notice filed stating that any party or nonparty could object.

Second, the Court must consider less drastic alternatives such as redactions or limited sealing. Here, Amazon only seeks to redact a few lines of the hearing transcript involving highly sensitive security measures, which the Court should find is proper. Redacting these lines is the only means by which to preserve the confidentiality of the sensitive security measures discussed. *See*, *e.g.*, *Walker Sys., Inc. v. Hubbell, Inc.*, 188 F.R.D. 428, 429 (S.D. W. Va. 1999) (stating "[w]here . . . the information sought to be protected concerns documents that the parties in good faith believe contain trade secrets or other confidential information, and the orders are routinely agreed upon by the parties, such orders should be granted") (citing *Bayer AG & Miles,*

Inc. v. Barr Labs, Inc., 162 F.R.D. 456, 465 (S.D.N.Y. 1995); Fed. R. Civ. P. 26(c)). Given the nature of the information, as explained below in Section II, redacting these lines is the only means by which to guarantee protection of Amazon's security threat intelligence gathering measures.

Third, the Court must make specific findings, supported by the record, that justify sealing based on either the First Amendment or common law. It is well-settled that there is a public right of access to "judicial records." *See Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597 (1978). The public right of access may be based on the common law or the First Amendment. The common law right of access applies to "all judicial records and documents," while the First Amendment right of access applies "only to particular judicial records and documents" – such as exhibits filed in connection with plea hearings and sentencing hearings in criminal cases, and trial proceedings and dispositive motions in civil cases. *Stone v. Univ. of Maryland Med. Sys. Corp.*, 855 F.2d 178, 180–81 (4th Cir. 1988).

The Excerpts relate to Defendants' dispositive motions on summary judgment. Even where the First Amendment attaches on dispositive motions, courts still recognize that "private interests might also implicate higher values sufficient to override (or, in an alternative mode of analysis, to except the proceeding or materials at issue from) the First Amendment presumption of public access." *Level 3 Commc'ns, LLC v. Limelight Networks, Inc.*, 611 F. Supp. 2d 572, 580 (E.D. Va. Apr. 30, 2009). "For example, the Fourth Circuit has suggested that '[a] corporation may possess a strong interest in preserving the confidentiality of its proprietary and trade-secret information, which in turn may justify partial sealing of court records [under the First Amendment].'" *Benedict v. Hankook Tire Co. Ltd.*, 323 F. Supp. 3d 747, 755 (E.D. Va.

June 15, 2018) (alteration in original) (quoting *Doe v. Public Citizen*, 749 F.3d 246, 269 (4th Cir. 2014) (citing *Nixon*, 435 U.S. at 598)).

The Excerpts discuss one of Amazon's security intelligence gathering practices, the usefulness of which would be compromised if revealed to the public. Further, the general public would have little interest in the information because it was generated by, and relates to, the internal activities of private entities. *See, e.g., Crum & Crum Enters. v. NDC of Cal.,* No. 09-145 (RBK), 2011 U.S. Dist. LEXIS 24690, at *12 (D. Del. Mar. 11, 2011). In fact, the general public benefits from the information remaining private so that Amazon can continue to learn about, respond to, and mitigate security threats. Amazon will be unable to continue to use these measures if they are publicly disclosed. Accordingly, under the First Amendment standard, Amazon's strong interest in preserving the confidentiality of its defensive security measures justifies redacting the Excerpts from the September 30, 2021 hearing transcript.

II. AMAZON'S CONFIDENTIAL TECHNICAL SECURITY INFORMATION SHOULD BE SHIELDED FROM PUBLIC ACCESS.

A district court may order a filing to be sealed where it contains confidential business information. In fact, a corporation's confidential information is considered a type of property to which the corporation has an exclusive right and benefit. *See e.g.*, *Carpenter v. United States*, 484 U.S. 19, 26 (1987). The public right of access must give way to protect the confidential business information of parties in judicial filings. *See, e.g., Nixon*, 435 U.S. at 598; *In re Knight*, 743 F.2d at 235 (sealing court records is permissible to prevent others from "gaining a business advantage" from materials filed with court). District courts in the Fourth Circuit have generally followed this standard where the First Amendment attaches, sealing documents relating to a corporation's non-public financial information and other proprietary business and trade-secret information. *See, e.g., E.W., LLC v. Rahman*, 2012 WL 3843657, at *3

(E.D. Va. Sept. 4, 2012) (sensitive financial data, including gross profit data, the disclosure of which would be highly likely to cause significant harm to the company's competitive position).

In addition, courts that have considered the issue have sealed documents relating to a corporation's cybersecurity practices, reasoning that disclosing that information "could allow cyberattackers greater opportunity to defeat these defenses and substantially harm both [the corporation] and putative class members." *See, e.g.*, *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2018 WL 3092256, at *2 (N.D. Cal. Mar. 16, 2018) (citing *Bell v. Home Depot U.S.A., Inc.*, 2015 WL 6082460, at *2 (E.D. Cal. Oct. 15, 2015) (finding "compelling reasons" to seal documents that contained the defendant's "security protocols in opening and closing its stores, the disclosure of which could threaten its stores' security and its employees' safety")); *In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2013 WL 5366963, at *3 (N.D. Cal. Sept. 25, 2013) (granting motion to seal information on how Gmail operates and other information where "Google's ability to combat spammers, hackers, and others who propagate these unwanted or harmful materials would be impaired if those individuals had visibility into Google's defenses"); *id*. (noting that "there is no strong public interest in disclosure of the material regarding the effect of users' actions on Google's processing, since this material is unlikely to be critical to the substantive issue of liability").

The Excerpts here should likewise be sealed because they contain confidential technical and business information that could harm Amazon and its ability to gather intelligence on security threats if filed publicly. As Steve Schuster, Director of Security Engineering and Response with Amazon Web Services, Inc., explains in his Declaration in support of Amazon's Confidential Memorandum in Support of Motion to Seal (Dkt. 1992), the information contained in the Excerpts regarding Amazon's security threat intelligence practices is confidential and competitively sensitive. *See* Dkt. 1992 (Schuster Decl.) ¶ 2. Mr. Schuster attested that public

disclosure of this information could provide outsiders with non-public details about Amazon's cybersecurity practices, such as threat intelligence gathering efforts, and could therefore compromise Amazon's overall security as well as cause it competitive injury. *Id*. ¶¶ 2, 4. This is precisely the type of malicious behavior that the *In re Google* court noted when it allowed sealing of certain information about Gmail's operations. 2013 WL 5366963, at *3. Similarly here, the Excerpts describe Amazon's non-public, and current, threat intelligence practices. If information regarding the threat detection practices are released, every member of the public, including malicious actors, will have insight into Amazon's security infrastructure, defeating the purpose of the intelligence program. *See* Dkt. 1992 (Schuster Decl.) ¶¶ 2, 4. This ongoing and real threat means that Amazon's interest in protecting from public disclosure any information about its security intelligence gathering techniques outweighs the public's minimal interest, if any, in learning about those techniques unique to Amazon.

It appears that this Court agrees. At the September 10, 2021 hearing, this Court recognized that there is a "compelling government interest" in protecting information about "current architecture . . . so that bad actors can't go in and find out information that could assist them in further intrusions or other bad activities." Sept. 10, 2021 Hr'g Tr. 8:25-9:5.

CONCLUSION

In sum, protecting Amazon's confidential and highly sensitive security measures justifies sealing the Excerpts from the September 30, 2021 hearing. Dkt. 2030. Amazon respectfully requests that its Motion to Seal and Notice of Intent to Request Redaction of the September 30, 2021 hearing transcript be granted consistent with the attached proposed order.

November 3, 2021

Respectfully submitted,

/s/ Robert R. Vieth

Robert R. Vieth, Esq. (VSB No. 24304)
HIRSCHLER FLEISCHER, PC
8270 Greensboro Drive, Suite 700
Tysons Corner, VA 22102
T: (703) 584-8366
F: (703) 584-8901
Email: rvieth@hirschlerlaw.com

Local counsel for Defendants Amazon.com, Inc. and Amazon Web Services, Inc.

Tyler G. Newby (admitted *pro hac vice*)
Brian Buckley (admitted *pro hac vice*)
Laurence F. Pulgram (admitted *pro hac vice*)
Jedediah Wakefield (admitted *pro hac vice*)
Vincent Barredo (admitted *pro hac vice*)
Andrew M. Lewis (admitted *pro hac vice*)
Janie Y. Miller (admitted *pro hac vice*)
Meghan E. Fenzel (admitted *pro hac vice*)
Sarah V. Lightstone (admitted *pro hac vice*)
Rina Plotkin (admitted *pro hac vice*)
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: (415) 875-2300
Facsimile: (415) 281-1350
Email: tnewby@fenwick.com
bbuckley@fenwick.com
lpulgram@fenwick.com
jwakefield@fenwick.com
vbarredo@fenwick.com
alewis@fenwick.com
jmiller@fenwick.com
mfenzel@fenwick.com
slightstone@fenwick.com
rplotkin@fenwick.com

Counsel for Defendants Amazon.com, Inc. and Amazon Web Services, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on November 3, 2021, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ Robert R. Vieth
Robert R. Vieth, Esq. (VSB No. 24304)
HIRSCHLER FLEISCHER, PC
8270 Greensboro Drive, Suite 700
Tysons, Virginia 22102
T: (703) 584-8366
F: (703) 584-8901
Email: rvieth@hirschlerlaw.com

Local Counsel for Defendants Amazon.com, Inc. and Amazon Web Services, Inc.